

Feb 03, 2023

s/ D. Olszewski

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)Single-family residence and garage located at N3184
Evergreen Rd, Lake Geneva, WI 53147; the Black Infinite
QX80 SUV bearing WI license plate number "ARW2153"
located at N3184 Evergreen Rd, Lake Geneva, WI 53147;
and the person of James BUSHEY (See Attachments)

Case No. 23 MJ 3

Matter No.: 2021R00255

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure
of the following person or property located in the _____ District of _____

(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 2/17/2023 (not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to _____

Honorable William E. Duffin

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 2/3/2023 at 1:56 PM



Judge's signature

City and state: Milwaukee, WI.

Honorable William E. Duffin, Magistrate Judge

Printed name and title

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A
Property and Person to Be Searched

- The single-family residence and garage located at N3184 Evergreen Rd, Lake Geneva, WI 53147. This residence is described as a two-story residence with green siding and an attached garage. The residence has a driveway that consists of both cement and brick, and to the south of the drive is a blue colored fire sign with “N3184” posted on it. The residence is located on the east side of Evergreen Road;
- Black Infinite QX80 SUV bearing WI license plate number “ARW2153” located at N3184 Evergreen Rd, Lake Geneva, WI 53147; and
- The person of James BUSHEY

ATTACHMENT B
Particular Items to Be Seized

1. All records relating to violations of 18 U.S.C § 371 (Conspiracy); 18 U.S.C. 922(l) (Illegal Import of Ammunition); 18 U.S.C § 542 (Entry of Goods by Means of False Statements); 18 U.S.C. § 545 (Smuggling); and impersonating an officer or employee of the United States (18 U.S.C. § 912), those violations involving Darin DOWD, Jacob DOWD, Eli LAZAR, James BUSHEY and others and occurring after January 1, 2020, including:

- a. Records related to firearms, ammunition, firearm accessories, to include pistols, handguns, shotguns, rifles, machine guns, silences, NFA weapons, magazines;
- b. Records and information relating to a conspiracy to defraud the ATF and the government;
- c. Records relating to firearm and ammunition purchases, contracts, transfers, sales, travel, and shipments
- d. Records relating to any ATF forms or firearm or ammunition licensing;
- e. Records and information relating to UFE firearm and ammunition purchases, contracts, transfers, sales, travel, and shipments;
- f. Records related to the impersonation of law enforcement, including federal ATF agents;
- g. Records related to financial transactions and travel records for UFE owners, employees, and associates;
- h. Records and information relating to the e-mail and social media accounts connected to UFE, Darin DOWD, Jacob DOWD, James BUSHEY, and Eli LAZAR;
- i. Records and information relating to the identity or location of the suspects;

- j. Records and information relating to communications with Internet Protocol addresses;
- k. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- l. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);
- m. The contents of all emails associated with the account from 02/12/18 to present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses

associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

- n. The contents of all instant messages associated with the account 02/12/18 to present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;
- o. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;
- p. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases,

downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

- q. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;
- r. All records pertaining to the types of service used;
- s. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and
- t. Records related to all files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web

pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of James BUSHEY to the fingerprint scanner of the device; (2) hold a device found in front of the face of James BUSHEY and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

Feb 03, 2023

s/ D. Olszewski

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the

IN THE MATTER OF THE SEARCH OF

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Single-family residence and garage located at N3184 Evergreen Rd,
Lake Geneva, WI 53147; the Black Infinite QX80 SUV bearing WI
license plate number "ARW2153" located at N3184 Evergreen Rd,
Lake Geneva, WI 53147; and the person of James BUSHEY (See
Attachments)

Case No. 23 MJ 3

Matter No.: 2021R00255**APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 371 and 922(i), 542, 545	Conspiracy; Illegal Import of Ammunition; Entry of Goods by Means of False Statements; Smuggling; and impersonating an officer or employee of the United States

The application is based on these facts:

See attached affidavit.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

RICHARD CONNORS

Digitally signed by RICHARD CONNORS
Date: 2023.02.02 15:58:35 -06'00'

Applicant's signature

SA Richard E. Connors III, ATF

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
 _____ telephone _____ (specify reliable electronic means).

Date: 2/3/2023



Judge's signature

City and state: Milwaukee, WI.

Honorable William E. Duffin, Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Richard Connors, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the premises and the person listed under Attachment A, for the things described in Attachment B. The premises and person in Attachment A follow:

- The single-family residence and garage located at N3184 Evergreen Rd, Lake Geneva, WI 53147;
- Black Infinite QX80 SUV bearing WI license plate number “ARW2153” located at N3184 Evergreen Rd, Lake Geneva, WI 53147; and
- The person of James BUSHEY

2. I am employed as a Special Agent with the United States Department of Justice, Bureau of Alcohol, Tobacco, Firearms, and Explosives (“ATF”) assigned to the Milwaukee Field Office since October of 2015. I have been employed as a full-time law enforcement officer for approximately seven years. I have received training at the Federal Law Enforcement Training Center in Glynco, GA. I attended the Criminal Investigator Training Program, as well as ATF’s Special Agent Training Program. I have received training in the investigation of unlawful possession of firearms, the unlawful transfer of firearms, and the unlawful dealing in firearms without a dealers’ license. Prior to becoming a Special Agent with the ATF, I received two bachelor’s degrees from Northern Illinois University in the fields of Sociology and International

Relations. I have received a master's degree from Northern Illinois University in the field of American Government.

3. I have received training in the investigation of firearm trafficking. Based on my training, experience, and participation in firearm trafficking investigations, I know and/or have observed the following:

- a. I have utilized informants to investigate firearm trafficking. Through informant interviews and debriefings of individuals involved in those offenses, I have learned about the manner in which individuals and organizations distribute firearms in Wisconsin and elsewhere;
- b. I have also relied on informants to obtain firearms from individuals on the streets (as opposed to licensed gun dealers), via what are known as a controlled purchases;
- c. I have experience conducting street surveillance of individuals engaged in firearm trafficking. I have participated in the execution of numerous search warrants where firearms, ammunition, and magazines have been seized;
- d. I am familiar with the language utilized over the telephone to discuss firearm trafficking, and know that the language is often limited, guarded, and coded;
- e. I know that firearm traffickers often use electronic equipment to conduct these operations; and
- f. I know that firearm traffickers often use proceeds to purchase assets such as vehicles, property, jewelry, and narcotics. I also know that firearm and drug traffickers often use nominees to purchase and/or title these assets to avoid

scrutiny from law enforcement officials. I also know what firearm and drug traffickers may keep photographs of these items on electronic devices.

4. I have participated in multiple firearm and drug trafficking investigations that involved the seizure of computers, cellular phones, cameras, and other digital storage devices, and the subsequent analysis of electronic data stored within these computers, cellular phones, cameras, and other digital storage devices. On many occasions, this electronic data has provided evidence of the crimes being investigated and corroborated information already known or suspected by law enforcement.

5. The facts in this affidavit come from my personal observations, my training and experience, and from information obtained from other investigators and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C § 371 (Conspiracy); 18 U.S.C. 922(l) (Illegal Import of Ammunition); 18 U.S.C § 542 (Entry of Goods by Means of False Statements); 18 U.S.C. § 545 (Smuggling); and impersonating an officer or employee of the United States (18 U.S.C. § 912) have been committed and that evidence of those violations may be located at the locations described in Attachment A.

7. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

PROBABLE CAUSE

9. The facts set forth in the affidavit below will display that there is probable cause to believe that the owners and associates of United Forces Enterprises, a federal firearms licensee

(FFL), conspired with a former police chief and members of the public to lie on an ATF Form 6 (ATF Official importation form) for monetary gain. The sole owners of United Forces Enterprises have been identified as Jacob DOWD (DOB: 1993) and Darin DOWD (DOB: 1991), brothers, who are originally from the Sacramento, CA, area. United Forces Enterprises possesses the following ATF Licenses: 01-Dealer License, 09-Dealer in Destructive Devices, 08-Importer Firearms License, and 11-Importer of Destructive Devices. These licenses are regulated by ATF and allow United Forces Enterprises the lawful ability to conduct certain transactions both domestically and internationally. The address on the licenses for United Forces Enterprises is listed as 2581 Nut Tree Road, Suite A, Vacaville, CA, 95687. Jacob and Darin DOWD utilized their FFL to conduct certain lawful transactions during the duration of their licensure. ATF became aware of potential misconduct by United Forces Enterprises when a suspicious ATF Form 6 was submitted via Jacob DOWD to the ATF imports branch. The facts raised in this affidavit will display that the DOWDS, along with several of their co-conspirators, conspired to violate United States Federal law.

10. This investigation has been supported by several interviews; approximately twenty-three grand jury subpoenas for various bank, cell phone, and other electronic records; and three federal search warrants for various electronic communications. On 11/03/2021, ATF Special Agent Ryan Arnold obtained a Google search warrant for the GMAIL accounts “UnitedForcesEnterprises@gmail.com,” “Darindowdjr@gmail.com,” “A.elilazar@gmail.com,” and “ATYPTC@gmail.com.” On 11/19/2021, your affiant obtained a federal search warrant for the Apple iCloud account associated with Darin DOWD listed as “darin.dowd@iCloud.com.” Lastly, on 01/03/2022, your affiant obtained an Apple iCloud account search warrant for the account associated with Jacob DOWD listed as “jakedowd@iCloud.com.”

11. I reviewed the public website for United Forces Enterprises under URL <https://unitedforces.com/>. The website does not offer routine information as seen on traditional FFL and business websites such as contact information, a company overview, or profiles of staff. The website appears to consist of only a welcome page. On the page, it states the company is, “providing comprehensive solutions all over the world.”

12. Following the above statement, the website lists the following ten (10) types of ammunition. Each ammunition has an expandable section marked by a “+” sign and provides generic information about the selected round. For example, the expanded information under the 9x19 Luger simply advises the round is used for short range distances and recommend for matches or practice. There is no information on how to obtain this product.

13. The website listed the following entities as partnered brands:
- ZVS Armory (an ammunition company located in Prievidza, Slovakia)
 - STV Group (which is the largest producer of ammunition in the Czech Republic <https://www.stvgroup.cz/en>)
 - Phoenix MN Ammunition (a private Romanian company that manufactures small caliber ammunition (<https://www.phoenixms.ro/about-us/>)
 - Sumbro (a Macedonian ammunition manufacturer)
 - ZSR (an ammunition and explosives company in Turkey <https://zsrpatlayici.com/EN>)

14. Although no contact information was found on the United Forces Enterprises website, an Instagram page for United Forces Enterprises was located at <https://www.instagram.com/unitedforcesenterprises/>. As with all Instagram pages, there is an option to send a direct message to the user. The page provides a link to the webpage www.unitedforces.com. This is a dead link as the actual webpage address is <https://unitedforces.com> as mentioned in the above paragraph. Further, the Instagram page provided photographs that appear to be taken from the Internet. There are no photographs of

employees, advertisements, or a business location provided. In my training and experience this is unusual for an FFL's social media page.

15. Your Affiant also reviewed the public website for Alpha Omega Brokerage (<https://aobrokerage.com/>). The site claimed Alpha Omega Brokerage is the exclusive broker for United Forces Enterprises. The site advertised Chris Kyle American Sniper Brand Ammunition that is distributed by United Forces Enterprises and provided a catalog for ordering the ammunition. The final three pages of the catalog were an order form, a copy of the Federal Firearms License (FFL) for United Forces Enterprises, and a copy of the State of California Ammunition Vendor License for United Forces Enterprises. The website listed the following subjects as employees:

- Eli Lazar – President
- Joshua Beske - Director of Logistics/Military Liaison

16. On April 29, 2021, the bank account for United Forces Enterprises (Jacob and Darin DOWD are additional names on the account) listed as Bank of America Account number 325081477609 had an outgoing wire transfer of \$793,266.00 to a company named Smart Energo Sistemi of Pale, Republika Srpska 71420, Bosnia and Herzegovina. This appears to be an ammunition broker or manufacturer located in Bosnia.

17. Agents eventually located a “note” within the iCloud account for Darin DOWD (dob: 1991). This note appeared to be a list of questions regarding the importation of ammunition. This “note” contained the creation date of May 5, 2021.

1. What countries is the Insured importing product from?
Czech/Macedonia/Bosnia/Turkey
2. What countries is the Insured exporting to? What % of sales is exports vs. domestic?
100% import no domestic

3. Any armor piercing ammo (except .22 caliber rimfire “green tip” ammo weighing 40 grains or less)?

No armor piercing rounds will ever be imported as it is illegal

4. Any “green tip” ammo other than .22 caliber rimfire weighing 40 grains or less?

No green tip rounds will ever be imported as it is illegal

5. Any incendiary ammo?

No incendiary ammo will be imported as it is illegal

6. Who tends to be the Insured’s customers?

The manufacture handles all insurance for shipping and product “CIF”

7. Does the insured keep records of when each product was bought, batch numbers, and then to whom and date of sales? How long are these records retained?

Yes by ISO regulations manufactures keep records of product. Unknown for how long they retain records overseas. UFE retains its own records via online backup software and hard copy records.

8. The insured will be required to receive Additional Insured endorsements from the manufacture/suppliers.

18. Questions three (3) and five (5) appear to reflect Darin DOWD answering questions regarding the legality of importing armor piercing ammunition. The answer to his question three (3) states “No armor piercing rounds will ever be imported as it is illegal.” The same answer followed up his question number five (5). These notes indicate that the DOWDS were aware that importing armor piercing and incendiary ammunition into the United States would be illegal.

19. Investigators reviewed text message conversations between Jacob and Darin DOWD dated June 10, 2021, these results were received through Jacob DOWD’s Apple iCloud account. The phone number for Darin DOWD had been identified as 209-996-1451. The below conversation occurred on June 10, 2021.

- Jakedowd@icloud.com: When do you need to depart/arrive in Wisconsin
- 209-996-1451 (DoubleD): What up g! I can depart tomorrow at any time and then come home Monday This place is insane
- Jakedowd@iCloud.com: KK on it Also should I sign contract?
- 209-996-1451 (DoubleD): Yes it’s a green light Just having John our attorney change verbiage

Investigators reviewed the below conversation which occurred on June 13, 2021.

- 209-996-1451 (DoubleD) What up g !!!
- Jakedowd@iCloud.com: Sup pimp!
- 209-996-1451 (DoubleD): In lake Geneva fuckin place reminds me of the Hampton's god damn

20. On June 20, 2021, investigators reviewed a conversation between the two brothers discussing payments made to individuals named "Jason and Josh." These individuals have been identified by ATF as Jason WIEDENHOEFT (DOB: 1977), and Joshua BESKE (DOB: 1980) of Alpha Omega Brokerage. Additionally, the DOWDS refer to an individual by the name of "Lucifer," who has been identified by ATF as Eli LAZAR (DOB: 1996). LAZAR is the owner of Alpha Omega Brokerage. The conversation is depicted below discusses a purchase order for cartridges or ammunition. WIEDENHOEFT and BESKE appear to be making a certain cent per round depending on the order they are referencing.

	DoubleD	
06/20/2021 13:17:57	(209) 996-1451 - DoubleD	With Jason and Josh
06/20/2021 13:18:10	(209) 996-1451 - DoubleD	Luci just got dumped
06/20/2021 13:18:27	jakedowd@icloud.com - Jacob Dowd	Lmao
06/20/2021 13:18:41	(209) 996-1451 - DoubleD	We can also mix cartridges
06/20/2021 13:18:50	jakedowd@icloud.com - Jacob Dowd	Fuck yea
06/20/2021 13:19:00	(209) 996-1451 - DoubleD	They can be whatever we want they don't care
06/20/2021 13:19:13	jakedowd@icloud.com - Jacob Dowd	Fuck yea!
06/20/2021 13:19:52	(209) 996-1451 - DoubleD	AO is having no part in it either just UFE Jason and Josh so smooth sailing
06/20/2021 13:20:09	(209) 996-1451 - DoubleD	Said if ATF needs anything changed on PO we can do whatever they ask
06/20/2021 13:22:58	jakedowd@icloud.com - Jacob Dowd	Fuck yea!
06/20/2021 13:24:12	(209) 996-1451 - DoubleD	So Jason said .10 per cartridge to him. I was like fuck it .04 more cents and I said that is final he can't change it he agreed. This is gonna bring in so much god damn money lol
06/20/2021 13:26:06	jakedowd@icloud.com - Jacob Dowd	Fuck that's a lot per cartridge G
06/20/2021 13:26:33	(209) 996-1451 - DoubleD	Yea it is .04 more cents but is it worth it?
06/20/2021 13:29:05	jakedowd@icloud.com - Jacob Dowd	I mean fuck we'll see
06/20/2021 13:29:25	jakedowd@icloud.com - Jacob Dowd	I thought .06 was real fuckin fair considering Luci only gets .01
06/20/2021 13:29:37	(209) 996-1451 - DoubleD	Luci isn't getting shit only Jason

21. On June 30, 2021, ATF Imports Branch flagged a suspicious ATF Form 6, Application for Permit and Importation of Firearms, Ammunition and Defense Articles submitted by Jacob Allen DOWD and Darin Wayne DOWD using an address of 2581 Nut Tree Road, Suite A, Vacaville, CA, 95687 and an email address of "unitedforceenterprises@gmail.com." An open-source search revealed this as the physical and email address of Federal Firearms Licensee (FFL)

United Forces Enterprises. The request was for the importation of 489,000 rounds of 7.62x 54mm armor piercing incendiary (API) rounds from Smart Energeo Sistemi in Pale, Bosnia and Herzegovina. Nonsporting ammunition may not be imported unless certain exceptions apply, including as relevant here for law enforcement use.

22. Your Affiant reviewed the application and observed the listed reason for importation was “LAW ENFORCEMENT SALES.” Consistent with that stated reason for importation, the application was submitted along with a law enforcement exemption letter from the Town of Linn, Wisconsin, Police Department (TLPD). The exemption letter took the form of a purchase order on TLPD letterhead and signed by TLPD Chief James BUSHEY (DOB: 1983) for 1.5 million rounds of 7.62x 54mm API ammunition. This furthered suspicions as TLPD is a very small department consisting of only six (6) full-time officers and five (5) reserve officers. TLPD sits on the edge of Lake Geneva, Wisconsin.

23. The application was digitally signed by “JACOB A DOWD” on 06/21/2021. The Form 6 listed “UNITEDFORCESENTERPRISES@GMAIL.COM” and “(707) 227-7590” as ways to contact DOWD. It should be noted Chief James BUSHEY signed the ammunition purchase order on 06/16/2021, exactly three days after Darin DOWD texted Jacob DOWD that he was in Lake Geneva.

24. Agents reviewed a conversation between Darin DOWD and Jacob DOWD via Jacob DOWD’s iCloud account dated 07/04/2021. The two discuss receiving an approved “form 6.” This refers to the ATF Form 6 which was discussed in paragraph twenty-one (21). Additionally, Darin DOWD states “Yea Jason gave me a personal guarantee from bushy he would push it thru.” Darin DOWD is referring to Jason WIEDENHOEFT and TLPD Chief James BUSHEY. The conversation is below:

07/04/2021 16:43:06	(209) 996-1451 - DoubleD	Hell yea thanks g money. Totally on brand. How is the Barnaul lookin?
07/04/2021 16:43:13	(209) 996-1451 - DoubleD	Bet we get approved form 6 this week
07/04/2021 16:43:25	(209) 996-1451 - DoubleD	Omg crypto is off the wall our strategy is fuckin tits
07/04/2021 16:43:50	(209) 996-1451 - DoubleD	
07/04/2021 16:43:51	(209) 996-1451 - DoubleD	Nothin like \$22,500 for round trip delta one tickets lol
07/04/2021 16:43:59	jakedowd@icloud.com - Jacob Dowd	Fuck yea traveling sounds money right now
07/04/2021 16:44:02	jakedowd@icloud.com - Jacob Dowd	Hahaha
07/04/2021 16:44:14	jakedowd@icloud.com - Jacob Dowd	I called wizards out hard
07/04/2021 16:44:22	jakedowd@icloud.com - Jacob Dowd	Yea form 6 should
07/04/2021 16:44:34	jakedowd@icloud.com - Jacob Dowd	Yea crypto gonna be sky rocketing in September
07/04/2021 16:44:38	(209) 996-1451 - DoubleD	Yea I mean if I'm not in Hawaii then I'm gonna be in Europe as much as possible
07/04/2021 16:44:43	(209) 996-1451 - DoubleD	What did you tell them?
07/04/2021 16:44:59	jakedowd@icloud.com - Jacob Dowd	100%
07/04/2021 16:45:04	jakedowd@icloud.com - Jacob Dowd	I'll send you screenshots
07/04/2021 16:45:11	(209) 996-1451 - DoubleD	Yea Jason gave me a personal guarantee from bushy he would push it thru

25. Agents reviewed a conversation between Darin DOWD and Jacob DOWD via Jacob DOWD's iCloud account dated 07/11/2021. The two discuss receiving an approved "form 6." This is referring to the ATF Form 6 which was discussed in paragraph twenty-one (21). Darin DOWD advised "I literally talked with Jason and Josh for fuckin 3 hours today They said Bushy guaranteed a form 6 this week Monday he is gonna call with his attorney into the ATF Savage." Additionally, Darin DOWD discusses Jason WIEDENHOEFT (dob: 1977) and Joshua BESKE (dob: 1980) wanting to cut ties with "Luci" who is Eli LAZAR (dob: 1996). Allegedly LAZAR referred to himself as a "Big bad arms dealer." The conversation is below:

07/11/2021 00:56:57	(209) 996-1451 - DoubleD	Hell yeal Spagos thought you went Mia dumb asses lol
07/11/2021 00:57:35	(209) 996-1451 - DoubleD	I literally talked with Jason and josh for fuckin 3 hours today
07/11/2021 00:58:25	(209) 996-1451 - DoubleD	They said bushy guaranteed a form 6 this week Monday he is gonna call with his attorney into the ATF
07/11/2021 00:58:27	(209) 996-1451 -	Savage

07/11/2021 01:01:13	jakedowd@icloud.com - Jacob Dowd	?????????
07/11/2021 01:01:18	jakedowd@icloud.com - Jacob Dowd	Holy shit lol
07/11/2021 01:01:29	jakedowd@icloud.com - Jacob Dowd	Gucci
07/11/2021 01:01:31	jakedowd@icloud.com - Jacob Dowd	Fuck yeaf
07/11/2021 01:07:43	(209) 996-1451 - DoubleD	Yea totally draining
07/11/2021 01:07:50	(209) 996-1451 - DoubleD	But worth if
07/11/2021 01:07:52	(209) 996-1451 - DoubleD	It
07/11/2021 01:08:08	(209) 996-1451 - DoubleD	Guess they both wanna ditch luci and be with us only
07/11/2021 01:08:43	(209) 996-1451 - DoubleD	Said luci is unstable and is caught up in lies about being a "big bad arms dealer" lol
07/11/2021 01:09:06	(209) 996-1451 - DoubleD	Got all the the info on clover too
07/11/2021 01:09:24	(209) 996-1451 - DoubleD	She is a freight forwarder just like robin
07/11/2021 01:10:05	(209) 996-1451 - DoubleD	She connects with arms dealers thru her custom broker and buys their ammo like a pimp and then sells it for them

26. On July 16, 2021, ATF agents traveled to Town of Linn Police Department to interview Chief James BUSHEY. In summary, Chief BUSHEY stated in August 2020 he was first visited in person by Jason WIEDENHOEFT (DOB: 07/1977) who identified himself as the salesman for United Forces Enterprises. WIEDENHOEFT worked for a different company that was contracted by United Forces Enterprises to secure these transactions (believed to Alpha Omega Brokerage). WIEDENHOEFT was a local individual whom the Chief had known for a

long time. WIEDENHOEFT and BUSHEY had also been roommates. Additionally, WIEDENHOEFT owns the Reaper Company, a nonprofit organization created to help veterans with PTSD, and Chief BUSHEY is on its board of directors.

27. Chief BUSHEY stated that WIEDENHOEFT advised Chief BUSHEY that United Forces Enterprises was a level ten (10) or level eleven (11) firearms dealer which allowed them to import firearms and ammunition from overseas. WIEDENHOEFT told Chief BUSHEY United Forces Enterprises were fulfilling large ammunition orders for Cabela's and other retailers which required the use of shipping containers. Chief BUSHEY reiterated that he had been told by several people this was "the gray area" the government worked under to acquire munitions.

28. WIEDENHOEFT explained his friend, known as "Josh" (suspected to be Joshua BESKE) worked as private security for the United Forces Enterprises leadership - *i.e.*, Darin DOWD and Jacob DOWD and travels with them on security details. Chief BUSHEY advised that BESKE was a Marine Scout Sniper. Chief BUSHEY advised that he met BESKE through WIEDENHOEFT and believed him to live in northern Wisconsin.

29. Chief BUSHEY also explained there was some unknown middleman completing these deals for United Forces Enterprises who introduced WIEDENHOEFT to the DOWDS. Agents believe this to be Eli LAZAR.

30. Chief BUSHEY reiterated that he was told by several people this was "the gray area" the government worked under to acquire munitions. He indicated all these multiple levels of assurances made him feel comfortable about the transaction. Chief Bushey figured if United Forces Enterprises was willing to give TLPD a \$20,000 donation then the company must have been legitimate.

31. Affiant reviewed the purchase order signed and authorized by Chief James

BUSHEY and dated June 16, 2021. The purchase order stated the following in summary:

- To: United Forces Enterprises, 2581 Nut Tree Road, Vacaville, Suite A, CA, 95687
- Order Date: 06/15/2021
- PO #: 00001
- Ship Date: 08/15/2021
- Order No. 1
- 7.62x54R API (armored piercing incendiary)
- Quantity: 1,500,000
- Cost: \$0

32. Your Affiant knows that a police department exemption letter (in this case the purchase order signed by the chief on department letterhead) is considered valid by ATF for two years. Therefore, the quantity on the purchase order can be filled in multiple purchases at different times. The exemption letter only expires for the importer after two years or the quantity listed is met.

33. Affiant reviewed the ATF Form 6s that corresponded to the Chief BUSHEY's purchase order for the 7.62x54R API rounds. The following information was provided in summary:

ATF Form 6 (Permit No. 202106103)

- Applicant Name: Jacob and Darin DOWD
- Address: 2581 Nut Tree Road, Suite A, Vacaville, CA, 95687
- Foreign Seller: Smart Energo Sistemi of Bosnia and Herzegovina
- Ammunition Submitted: 489,000 rounds of Steel Core, Armor Piercing Incendiary (API), 7.62x54R
- Purpose of Importation: Law Enforcement
- Digitally Signed: Jacob DOWD, President on 06/29/2021
- Telephone: 707/227-7590
- Email: UNITEDFORCESETERPRISES@GMAIL.COM

34. Chief BUSHEY stated that WIEDENHOEFT prepared the purchase order on fake

TLPD letterhead that WIEDENHOEFT mocked up. WIEDENHOEFT gave the purchase order to Chief BUSHEY to sign, and BUSHEY returned it to WIEDENHOEFT. Chief BUSHEY stated that he believed WIEDENHOEFT then passed the purchase order on to the DOWDS.

35. Chief BUSHEY also provided a second Linn Township Police Department Purchase Order that he did not sign that was requested by WIEDENHOEFT. The order listed a request for 3,000,000 rounds of 12.7X99 API Brass Case ammunition. This ammunition is commonly referred to in the United States as .50 caliber BMG, and “API” is an acronym for Armored Piercing Incendiary. This type of ammunition is used in firearms such as the Barrett M82 rifle and M2HB/M2 Browning belt-fed rifle. This is a large caliber weapon and is rarely, if ever, used for law enforcement purposes and even more rare to be an API round. The API 12.7x99 API round would be more commonly used in a firearm such as the M2HB/M2 belt-fed rifle. The purchase order listed the following information in summary:

- Order Date: 11/19/2020
- To: United Forces Enterprises, 2581 Nut Tree Road, Suite A, Vacaville, CA, 95687
- Description: 12.7x99 API Brass Case Ammunition
- Cost: \$0.00

36. Chief BUSHEY advised he was first contacted by ATF agents outside of the Eastern District of Wisconsin prior to this interview regarding the TLPD purchase order that accompanied the United Forces Enterprises ATF Form 6 import application.

37. Following their conversation, he and WIEDENHOEFT exchanged text messages regarding the ATF interaction beginning on June 30, 2021. WIEDENHOEFT advised Chief BUSHEY that ATF was going to call to ensure he approved the purchase order. On July 1, 2021, Chief BUSHEY told WIEDENHOEFT via text that ATF did call. WIEDENHOEFT asked Chief BUSHEY if the call was “an easy call or extensive” and explained he was “just curious so he could

tell others what to expect.” Chief BUSHEY advised WIEDENHOEFT that ATF advised the transaction “looked a bit odd that a small dept in WI was buying 1.5 million rounds of belt fed ammo.” Chief BUSHEY explained he told ATF “... well if you have a fleet or (*sic*) f16’s, then you’d know that is the minimum necessary to keep us going.” WIEDENHOEFT replied, “Lol we shall see the cali boys said that they have had no issues with ATF on this.” Affiant believes “cali boys” was a reference to Darin DOWD and Jacob DOWD. On July 14, 2021, Chief BUSHEY advised WIEDENHOEFT via text message that ATF agents were going to visit him that week. WIEDENHOEFT responded, “They’re gonna call ufe (United Forces Enterprises) right no me. Personally.” Chief BUSHEY explained it would be agents from Milwaukee and take less than an hour or hour and a half. WIEDENHOEFT and Chief BUSHEY exchanged the following text messages in summary:

- WIEDENHOEFT: Ok Should be routine I’m guessing
- WIEDENHOEFT: Should I make ufe available for a call
[Affiant knows from this investigation that UFE is United Forces Enterprises]
- Chief BUSHEY: Perhaps
- WIEDENHOEFT: I’m gonna get a hold of them now
- WIEDENHOEFT: What time they coming Friday
- Chief BUSHEY: Around noonish
- Chief BUSHEY: Ok
- WIEDENHOEFT: They are in Hawaii and probably would not look good legally if they were on the call he says this is routine as its a weird round. Plus the f 16 joke may have aroused them lmfao.
[Affiant knows from PayPal account information that packages have been addressed to Jacob DOWD in Kihei, Hawaii.]
- WIEDENHOEFT: Here is why the ammo
- WIEDENHOEFT: United Forces has surplus it doesn’t not need anymore overseas. Instead of it sitting in a warehouse they have offered to donate this surplus ammunition the Law enforcement community. This ammunition can be used for precision shooting training, traded for equipment or used at auction to raise money for the department.
- Chief BUSHEY: Ok sounds good

38. Chief BUSHEY stated that he consulted the attorney, James B. Duquette, who represents the TLPD, regarding the ammunition deal with the DOWDS. Chief BUSHEY stated that Duquette approved of the deal. But in a September 16, 2021 interview with the Affiant, Duquette stated that he offered no opinion on the legality of the proposed ammunition deal. He instead only offered an opinion regarding whether the police department could, as a matter of the law governing municipal contracts, enter an agreement to accept an ammunition donation. Duquette stated that he was under the impression the ammunition in question was to be used by the police department for training. He stated he never reviewed any of the documents in question. Chief BUSHEY did not tell Attorney Duquette that the agreement was that TLPD would receive a cash payment in exchange for Chief BUSHEY signing and submitting a purchase order falsely indicating that armor piercing incendiary ammunition was to be imported for TLPD law enforcement use.

39. Chief BUSHEY also stated that he consulted the Town of Linn Town Board, which approved of the deal. Affiant has reviewed audio recordings of the Town of Linn Board meeting and a Protective Services Committee meeting that preceded it. Chief BUSHEY ultimately received approval from the Town Board to do the deal he described. The Town Board approved what was described to them as an agreement between the TLPD and a California FFL for the FFL to donate ammunition to the TLPD. Chief BUSHEY did not tell the Town Board or its Protective Services Committee that the agreement was that TLPD would receive a cash payment in exchange for Chief BUSHEY signing and submitting a purchase order falsely indicating that armor piercing incendiary ammunition was to be imported for TLPD law enforcement use.

40. Chief BUSHEY also stated that he sought approval from ATF before submitting

the purchase order. Chief BUSHEY did call ATF Industry Operations Inspector (IOI) Miguel Ruiz. During that call, Chief BUSHEY described a donation agreement very much like the agreement he described to the Town of Linn Board and Attorney Duquette. IOI Ruiz stated that Chief BUSHEY asked him if he could accept a donation of ammunition from UFE. IOI Ruiz advised Chief BUSHEY he was not certain if it was legal to accept a donation, but believed it was poor optics for a police chief to engage in that behavior.

41. Your affiant located an email thread from Darin DOWD and the GMAIL account listed to the DOWDS and United Forces Enterprises and an individual employed by Ammo Inc. Ammo Inc. is an ammunition manufacture/re-sale corporation located in Scottsdale, AZ. The email thread was dated 08/02/2021. The contents discussed Darin DOWD offering to sell Ammo Inc. API (armor-piercing-incendiary) ammunition. The conversation is below:

- From: Darin Dowd <darin@unitedforces.com>
Sent: Monday, August 2, 2021 8:36 AM
To: Anthony Tate <anthony@ammo-inc.com>
Cc: Jacob Dowd <unitedforcesenterprises@gmail.com>
Subject: Re: 7.62x39 Stateside

Anthony,

I appreciate the quick response and adjusted PO. Attached is the signed copy. I apologize for the miscounted quantity on my end. Did you get a chance to look at the 308 GGG? Also, does Ammo Inc take surplus API calibers?

Thank you,

Darin Dowd
Vice President, United Forces Enterprises
CAGE Code: 7WBA5
DUNS #: 080748836
Cell Phone: 1(916) 546-6309
Office: 1(707) 227-7590
darin@unitedforces.com
- On Aug 2, 2021, at 7:35 PM, Anthony Tate <anthony@ammo-inc.com> wrote:

I have looked at the GGG - Give me a day or two on that one. Can you send me a list of the API

Anthony Tate | Director
National Accounts | Ammo Incorporated

anthony@ammo-inc.com | (928) 308 - 4731 |
www.ammo-inc.com

- On Aug 2, 2021, at 8:04 PM, Darin Dowd <darin@unitedforces.com> wrote:

Anthony,

No rush on the 308 Win whenever you get around to it is fine. API would be in calibers of 7.62x39, 7.62x54, 7.62 x 51 and 556x45 API. All terms would be COD.

Thank you,

Darin Dowd
Vice President, United Forces Enterprises
CAGE Code: 7WBA5
DUNS #: 080748836
Cell Phone: 1(916) 546-6309
Office: 1(707) 227-7590
darin@unitedforces.com

...

WARNING: If you take or ship guns, gun parts, optical sights, reloading components, or any controlled items under Bureau of Industry & Security (BIS)/Export Administration Regulation (EAR), International Traffic in Arms Regulations (ITAR) & Foreign Trade Regulations (FTR) out of the U.S., you must have prior approval from the appropriate U.S. Government agencies.

- From: Darin Dowd <darin@unitedforces.com>
Sent: Monday, August 2, 2021 12:03 PM
To: Anthony Tate <anthony@ammo-inc.com>
Cc: Jacob Dowd <unitedforcesenterprises@gmail.com>
Subject: Re: 7.62x39 Stateside

Anthony,

Also on all all API ammunition it would be a few months to delivery. Just wanted to see your interest on it.

Thank you,

Darin Dowd
Vice President, United Forces Enterprises
CAGE Code: 7WBA5
DUNS #: 080748836
Cell Phone: 1(916) 546-6309
Office: 1(707) 227-7590
darin@unitedforces.com
...

WARNING: If you take or ship guns, gun parts, optical sights, reloading components, or any controlled items under Bureau of Industry & Security (BIS)/Export Administration Regulation (EAR), International Traffic in Arms Regulations (ITAR) & Foreign Trade Regulations (FTR) out of the U.S., you must have prior approval from the appropriate U.S. Government agencies.

- On Aug 2, 2021, at 10:30 AM, Anthony Tate <anthony@ammo-inc.com> wrote:
I may have some interest. Please send me any details such as Specs and Pricing
Anthony Tate | Director
National Accounts | Ammo Incorporated
anthony@ammo-inc.com | (928) 308 - 4731 | www.ammo-inc.com

42. Agents reviewed a conversation between Darin DOWD and Jacob DOWD via Jacob DOWD's iCloud account dated 08/26/2021. The two discuss receiving an approved "form 6." This is referring to the ATF Form 6 which was discussed in paragraph twenty-one (21). They two discuss Chief James BUSHEY and the approved Form 6. The entire conversation is below:

08/26/2021 22:54:21	jakedowd@icloud.com - Jacob Dowd	Have we heard anything from Bushes
08/26/2021 22:54:25	jakedowd@icloud.com - Jacob Dowd	Bushey
08/26/2021 22:54:32	jakedowd@icloud.com - Jacob Dowd	It's been over 45 days on the form 6

08/26/2021 23:00:31	(209) 996-1451 - DoubledD	I was just thinking that when boats drive by (shitty boats) they point at the house big fuck you fountains fuckin hilarious
08/26/2021 23:00:50	(209) 996-1451 - DoubledD	Big day on stocks tomorrow also gonna get bravo echo to commit
08/26/2021 23:00:57	(209) 996-1451 - DoubledD	Are those same ship dates for 9mm?
08/26/2021 23:01:11	(209) 996-1451 - DoubledD	Can you send me quantity ship dates on 9mm
08/26/2021 23:02:06	(209) 996-1451 - DoubledD	Yea we did today I talked to Jason all approved on form 6 we just have to change it to .50 cents a round on PO and do a NET 180 with department and ATF will clear it they just didn't like \$0 for the product
08/26/2021 23:04:04	jakedowd@icloud.com - Jacob Dowd	Haha fuckin love it
08/26/2021 23:04:09	jakedowd@icloud.com - Jacob Dowd	Fuck yea
08/26/2021 23:04:17	jakedowd@icloud.com - Jacob Dowd	Yea same dates
08/26/2021 23:04:27	jakedowd@icloud.com - Jacob Dowd	9mm is same as 223
08/26/2021 23:04:46	jakedowd@icloud.com - Jacob Dowd	Ok good to know
08/26/2021 23:05:02	(209) 996-1451 - DoubledD	Ok perfect! Easy to copy
08/26/2021 23:05:49	(209) 996-1451 - DoubledD	Yea that was the only hang up they said the everything else was good. I have a conference call with bushey and Jason Sunday before they resubmit on Monday if you wanna hop on you can or I can just handle it
08/26/2021 23:06:56	jakedowd@icloud.com - Jacob Dowd	Yea I'll hop on
08/26/2021 23:07:19	(209) 996-1451 -	Ok cool I set it up for 3pm my tome

43. Your Affiant interviewed Jason WIEDENHOEFT on September 3, 2021, after WIEDENHOEFT called and asked to speak about ammunition sales. WIEDENHOEFT stated that he had worked for Eli LAZAR selling ammunition for LAZAR's company, Alpha/Omega Brokerage. WIEDENHOEFT stated that Alpha Omega Brokerage, in turn, was hired by two brothers in California, Jacob and Darin DOWD to sell ammunition on behalf of their FFL (United Forces Enterprises).

44. WIEDENHOEFT stated that he was on a conference call with the DOWDS and LAZAR in which the DOWDS explained that they needed law enforcement contacts in order to be able to import certain “specialty ammo” that they could not otherwise legally import. WIEDENHOEFT stated that LAZAR was not then involved in any law enforcement deals and that WIEDENHOEFT stated he could arrange a deal through his friend, TLPD Chief BUSHEY. He also stated that he does not like LAZAR and does not believe he is a good person.

45. WIEDENHOEFT stated that he believed that once a police department ordered ammunition, including specialty ammunition, it could barter it. But Affiant asked WIEDENHOEFT if the DOWDS needed a law enforcement agency to indicate that the purchase order was for them because of the ammunition’s armor piercing incendiary designation, and WIEDENHOEFT replied “correct.”

46. WIEDENHOEFT stated that “when I was first approached to sell, I was like this just doesn’t sound right. You know, because I’m skeptical and, if it sounds too good to be true, but it was, everything is legit.”

47. After the initial, in-person interview was completed, WIEDENHOEFT called the Affiant and stated that the DOWDS told him during the initial conference call that it was necessary to acquire an exemption letter in order to import incendiary rounds. WIEDENHOEFT stated that he believed only law enforcement could import incendiary rounds, though he believed anyone could buy them.

48. WIEDENHOEFT stated that he prepared the template that BUSHEY used for the purchase order, and that BUSHEY emailed him the signed agreement. He stated he believes he FedExed the agreement to the DOWDS.

49. WIEDENHOEFT stated that he was paid by the DOWDS through LAZAR’s

company, Alpha Omega Brokerage.

50. WIEDENHOEFT made no mention of James COMPSTON during his interview – apparently willfully - even when asked directly if anyone else was involved with him in law enforcement ammunition deals. Shortly after the interview with ATF, WIEDENHOEFT contacted the phone number 916-546-6309 on fourteen (14) occasions via text message. This phone number contains an area code for the Vacaville, CA, area.

51. Your affiant submitted a toll record/subscriber information subpoena to Verizon Wireless for the above number on 11/3/21. Your affiant received the records for the number 916-546-6309 on 11/8/21. The subscriber for the phone number is listed as Darin DOWD with an address of 7660 Hillhaven CT, Antelope, CA. Additionally, Verizon provided the email address for DOWD as darin.dowd@iCloud.com.

52. On September 15, 2021, Affiant interviewed James COMPSTON. Agents had contacted COMPSTON, and he invited agents to his home for the interview.

53. COMPSTON advised he was previously an Ohio State Trooper and was a member of the Columbus, Ohio, Federal Bureau of Investigation (FBI) Joint Terrorism Task Force (JTTF) in 1998.

54. COMPSTON told agents he spoke with “Jason” (agents know this to be Jason WIEDENHOEFT) before the agents arrived. He advised WIEDENHOEFT was his partner in these ammunition deals. COMPSTON knew WIEDEHOEFT was interviewed by ATF approximately two (2) weeks ago. COMPSTON stated that WIEDENHOEFT told him: “Make sure you tell the ATF that I forgot to mention your name [during ATF’s interview of WIEDENHOEFT], it wasn’t intentional.”

55. COMPSTON explained the agreed upon payment structure to agents. He advised

that he was to split all sales 50/50 with WIEDENHOEFT no matter who closed the deal. This split was drawn from a 10 cents per round sale price. COMPSTON would have received a share from the Town of Linn Police Department deal with Chief BUSHEY.

56. COMPSTON stated that WIEDENHOEFT emailed him a purchase order to use with other departments and that COMPSTON proposed the purchase-order-for-donation exchange agreement to other police departments but had no takers.

57. COMPSTON stated that he had previously emailed with LAZAR but that he had deleted the email account he used to do so. He stated that he did not email with the DOWDS or WIEDENHOEFT.

58. COMPSTON also stated that he never directly corresponded with the DOWDS, and that they instead initially only corresponded with LAZAR but later corresponded directly with WIEDENHOEFT.

59. COMPSTON said that, in his view, U.F.E. (which he sometimes referred to as “HFE”) would not bother to bring in 9mm, .40, .45, .308, 7.62x39 ammunition (*i.e.*, non-specialty ammunition) by using law enforcement exemption letters because they can bring it in without law enforcement.

60. Your affiant believes based on the previous information there was a detailed conspiracy to lie on an ATF Form 6 between Jacob and Darin DOWD, Eli LAZAR, Jason WIEDENHOEFT, and Chief James BUSHEY purely for monetary gain. As outlined above, Darin DOWD knew he could not lawfully import armor piercing incendiary ammunition back on 05/05/2021. Darin DOWD wrote down this information in the “notes” section of his presumed iPhone. This occurred after United Forces Enterprises paid a company in Bosnia \$793,266.00 for presumed ammunition. The same company, listed on the ATF Form 6 filed by Jacob DOWD to

the ATF back on 06/21/2021. The DOWDS presumably devised a plan with LAZAR, WIEDENHOEFT, and Chief James BUSHEY to import their API ammunition so they would not take a loss on what they already had paid on 04/29/2021. That plan involved recruiting a police chief to lie on an official purchase order claiming API ammunition was for a department which had no use for that particular round of ammunition. Of note, the ammunition would only be lawfully imported if it were for a law enforcement or military entity.

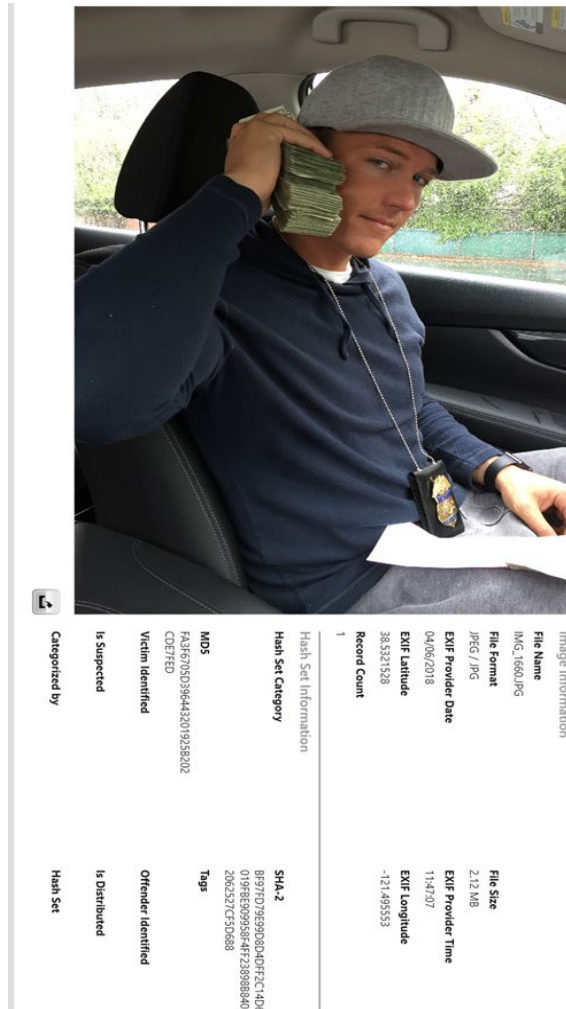
61. Your affiant is aware the bulk of the evidence against the subjects involved in the conspiracy is digital information likely stored on cell phones and or computers. Your affiant is requesting the search warrant be approved primarily for the search and recovery of digital evidence which will further prove the case against the DOWDS, WIEDENHOEFT, LAZAR, and BUSHEY.

INFORMATION CONCERNING THE IMPERSONATION OF ATF AGENTS

62. Agents searched through the iCloud return for Darin DOWD and located concerning information regarding the impersonation of ATF agents by the DOWDS. The events all appear to have occurred in the Sacramento, California area.

63. Agents observed a video of the DOWD brothers getting into a physical altercation with unknown individuals on or about 2/12/2018. The altercation is believed to have occurred at Syntrol Heating, Air, Plumbing, Electricity, Solar at 2120 March Rd a, Roseville, CA. During the video, one of the DOWD brothers can be heard stating "I'm a federal fucking agent, you're done." In the next video, one individual is heard stating "we can arrest them it's all good," "I'm an ATF Special Agent," and "Put your hands behind your back."

64. Further, the below photo depicts Darin DOWD with a fictitious ATF badge around his neck and was believed to be taken on 04/06/2018:



65. Agents observed a video in which Darin DOWD can be heard talking to Jacob DOWD. The video depicts Jacob DOWD firing a Berretta handgun while wearing a “ATF Special Response Team” T-Shirt. Agents confirmed neither Jacob nor Darin DOWD have ever been employed with the ATF. Additionally, agents spoke with a member of the actual ATF Special Response Team who confirmed the shirt in the video had not been issued to team members in recent history. The video was captured on 07/29/2018 and a screenshot is depicted below:



66. Your affiant was made aware of a witness named Nickolas Kokkos. Kokkos is a convicted felon who resides in the Sacramento, CA, area. In November 2018, KOKKOS contacted the ATF office in CA, and reported that an individual named Jacob DOWD of United Forces Enterprises LLC, had represented himself as an ATF agent and pressured Kokkos under the threat of arrest to sign papers releasing ownership of multiple firearms held in the custody of Sacramento Police Department to United Forces Enterprises. Kokkos admitted that his residence had been searched by the probation office that supervised him and that unregistered assault weapons were confiscated due to his felony conviction. After his case was resolved, two unknown white males drove to his house in a black SUV. The white males claimed to be ATF agents and told Kokkos he had to sign over custody of his firearms otherwise he would be detained. Kokkos stated one of the males displayed an ATF Badge and stated a “Notary” could arrive to witness him signing over the firearms. This same individual was armed with an apparent Sig Sauer handgun. Kokkos advised the second unknown white male was dressed like “Men in Black,” and possessed a Beretta

handgun (see above paragraph of Jacob DOWD firing Beretta handgun). One of the males had Kokkos sign a Sacramento Police Department Property release form and the same male called a Notary who arrived at his house. Kokkos stated he signed over his firearms out of fear of being arrested and the firearms were worth a lot of money.

67. Kokkos stated one of the males left a business card with the business name being “Solar Bros.” This is a known former business of the DOWD brothers. Additionally, the owner of the “Solar Bros” as listed on this business card was Jacob DOWD with a phone number of 209-675-6757. The address of the Solar Bros is 2581 Nut Tree Rd, Suite A, Vacaville, CA (the same address that used by UFE). Lastly, Kokkos provided ATF Special Agent Daniel Bietz a copy of the County of Sacramento Sheriff’s Department “Sale of Transfer of Firearm(s) Pursuant TO Penal Code Sections 12070 OR 12078(c)” form. The listed entity taking custody of the firearms from Kokkos on this form is listed as United Forces Enterprises at 2581 Nut Tree Rd, Suite A, Vacaville, CA, and the name of the dealer/agent is Jacob DOWD.

68. Your affiant is aware that in California if an individual has their firearms seized by a law enforcement official, that prohibited person can request their firearms be released to a Federal Firearms Licensee for re-sale and re-coup some of the monetary loss of losing those firearms. It appears as if Jacob DOWD attempted to blatantly steal Mr. Kokkos’s firearms once they had been lawfully seized by the Sacramento Sheriff’s Department under the guise of him being an ATF agent.

69. Your affiant located several notes and messages of the DOWDs seeking out individuals who had their firearms seized by police. The messages/notes were located within the Darin DOWD iCloud return. The behavior was documented between 10/15/2017 and 03/16/2020. Some of the notes located are depicted below:

- “Have you been convicted of a Felony and had your firearms confiscated? Henderson V. United States 1967 ruled that convicted felons can transfer their confiscated firearms to a third party rather than relinquishing them to the government, as long as the third party has their FFL license and is cleared by the ATF. We can help you transfer your confiscated firearm (s) out of the hands of the government and we will donate money for every firearm transferred. Call, text, or Email us today for more information”
- The following message was observed on 11/08/2018: “Get money for confiscated Guns! If you or someone you know have had their guns confiscated in California, we can help you earn money with your guns that you will never get back anyways! Call or text today and find out how.”

70. Your affiant observed multiple iCloud entries dated 11/15/2018 depicting firearms seized from various individuals. Additionally, the DOWDS’ saved photographs from either police or news sources of firearm seizure.

71. Your affiant reviewed bank information from the UFE checking account under Bank of America account number 325081477609. Your affiant observed the checking account 325081477609 received multiple wires from SSL Firearms located at 601 Gordon Industrial Ct SW, Byron Center, MI, 49315. Their website suggests SSL Firearms specializes in firearm and ammunition auctions.

72. The first payment from SSL firearms was wired to UFE’s checking account on 04/22/2019, for \$41,837.43. The memo line for the wire transfer stated, “Auction Payout Paid In Full.” There were twenty-seven (27) incoming wire transfers from SSL Firearms to UFE between the dates of 04/22/2019 and 02/01/2022. The total amount of money broken up over those transfers was \$688,882.87. Your affiant is aware UFE, and the DOWD brothers were actively looking for firearms seized from convicted felons in and around California.

BUSHEY’S RESIDENCE IN THE EASTERN DISTRICT OF WISCONSIN

73. Affiant is aware James BUSHEY’s current driver’s license in the state of Wisconsin

has the listed address of N3184 Evergreen Rd, Lake Geneva, WI 53147. Additionally, agents observed BUSHEY's listed address in a commonly utilized law enforcement database to be N3184 Evergreen Rd, Lake Geneva, WI 53147. On 02/02/2023 at approximately 0911 hours, law enforcement conducted surveillance on N3184 Evergreen Rd, Lake Geneva, WI 53147 and observed a black Infinite QX80 SUV parked in the driveway bearing WI license plate number "ARW2153". WI DOT records show that the aforementioned license plate is registered to James BUSHEY at N3184 Evergreen Rd, Lake Geneva, WI 53147.

CONCLUSION

74. Based on all the aforementioned information, your affiant believes there is probable cause to search James BUSHEY for the purpose of searching for electronic and paper documents related to the above stated crimes. Darin DOWD, Jacob DOWD, Eli LAZAR, Jason WIEFENHOEFT, and James BUSHEY appear to have conspired to lie on an ATF Form 6 to import API ammunition through the Town of Linn Police Department knowing the ammunition would not be delivered to the police department, and they used documents and electronics to further these crimes. This information is corroborated by the text messages, bank transfers, and emails laid out above. Your Affiant knows electronic devices are very likely to contain important evidence of the crimes described above, especially when the co-conspirators routinely communicate via cell phone. Evidence of the crimes described in the beginning of this affidavit is very likely to be contained on the electronic devices used by the identified co-conspirators. Your affiant believes that Jacob DOWD, Darin DOWD, Jason WIEDENHOEFT, Eli LAZAR, James COMPSTON, and James BUSHEY agreed to submit and did submit an ATF Form 6 with a false statement of reason for import along with a purchase order that falsely indicated a law enforcement

entity sought to purchase imported armor piercing incendiary ammunition. They intentionally did so to thwart the ban on the importation of that ammunition for their purposes.

75. Your affiant further believes that the Jacob DOWD, Darin DOWD, Jason WIEDENHOEFT, Eli LAZAR, James COMPSTON, and James BUSHEY attempted to illegally import armor piercing incendiary ammunition despite knowing it was illegal to do so.

76. Your affiant further believes that Jacob DOWD and Darin Dowd have engaged in an ongoing scheme to commit structuring, embezzlement, money laundering, and tax evasion. Evidence of these crimes is very likely to be contained on the electronic devices used by the identified co-conspirators and present at the locations identified in Attachments A.

77. That Affiant knows that businesses, such as FFLs, who sell ammunition and firearms commonly maintain photographs, documents, communication regarding the purchase and/or sale of those items on remotely stored accounts such as Apple and within email accounts maintained by Apple such as “iCloud.” Further, these communications can contain messages regarding the scheme. It can also reveal travel key to identifying other regions and municipalities that have been approached to participate. This is further corroborated by the slew of information obtained in the aforementioned iCloud returns from Jacob and Darin DOWD.

78. That based upon Affiant’s training and experience, Affiant knows that the execution of a search warrant related to remotely stored accounts such as Apple and within email accounts maintained by Apple such as “iCloud”, bank statements, photographs, videos, and other items or documents which establish the identities of persons in control of the media.

79. That based upon Affiant’s training and experience, Affiant knows that individuals purchasing and selling firearms routinely keep emails regarding the purchases and/or sales.

80. That Affiant knows that it is common for firearms purchasers to maintain electronic records, receipts, notes, ledgers, receipts relating to the transportation, ordering and purchase of firearms and that such records are typically kept where the purchaser would have ready access to them including Apple accounts.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

81. As described above and in Attachment B, this application seeks permission to search for records that might be found on the persons and locations described in Attachment A, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

82. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active

file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

e. Based on actual inspection of other evidence related to this investigation, spreadsheets, financial records, invoices, I am aware that computer equipment was used to generate, store, and print documents used in the above-described scheme. There is reason to believe that there is a computer system currently located on the persons and at the locations described in Attachment A.

83. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium on the persons and at the locations described in Attachment A because:

a. Data on the storage medium can provide evidence of a file that was once on the

storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain

information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion

is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

84. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the

warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

85. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

86. Because several people share the residential locations described in Attachment A

as a residence, it is possible that these locations will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

87. UFE (“the Company”) may be a functioning company that conducts business. The seizure of the Company’s computers may limit the Company’s ability to conduct its business. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and what computers or storage media need not be seized or copied. Where appropriate, officers will copy data, rather than physically seize computers, to reduce the extent of disruption. If employees of the Company so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of the Company’s legitimate business. If, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

ATTACHMENT A
Property and Person to Be Searched

- The single-family residence and garage located at N3184 Evergreen Rd, Lake Geneva, WI 53147. This residence is described as a two-story residence with green siding and an attached garage. The residence has a driveway that consists of both cement and brick, and to the south of the drive is a blue colored fire sign with “N3184” posted on it. The residence is located on the east side of Evergreen Road;
- Black Infinite QX80 SUV bearing WI license plate number “ARW2153” located at N3184 Evergreen Rd, Lake Geneva, WI 53147; and
- The person of James BUSHEY

ATTACHMENT B
Particular Items to Be Seized

1. All records relating to violations of 18 U.S.C § 371 (Conspiracy); 18 U.S.C. 922(l) (Illegal Import of Ammunition); 18 U.S.C § 542 (Entry of Goods by Means of False Statements); 18 U.S.C. § 545 (Smuggling); and impersonating an officer or employee of the United States (18 U.S.C. § 912), those violations involving Darin DOWD, Jacob DOWD, Eli LAZAR, James BUSHEY and others and occurring after January 1, 2020, including:

- a. Records related to firearms, ammunition, firearm accessories, to include pistols, handguns, shotguns, rifles, machine guns, silences, NFA weapons, magazines;
- b. Records and information relating to a conspiracy to defraud the ATF and the government;
- c. Records relating to firearm and ammunition purchases, contracts, transfers, sales, travel, and shipments
- d. Records relating to any ATF forms or firearm or ammunition licensing;
- e. Records and information relating to UFE firearm and ammunition purchases, contracts, transfers, sales, travel, and shipments;
- f. Records related to the impersonation of law enforcement, including federal ATF agents;
- g. Records related to financial transactions and travel records for UFE owners, employees, and associates;
- h. Records and information relating to the e-mail and social media accounts connected to UFE, Darin DOWD, Jacob DOWD, James BUSHEY, and Eli LAZAR;
- i. Records and information relating to the identity or location of the suspects;

- j. Records and information relating to communications with Internet Protocol addresses;
- k. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- l. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);
- m. The contents of all emails associated with the account from 02/12/18 to present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses

associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

- n. The contents of all instant messages associated with the account 02/12/18 to present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;
- o. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;
- p. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases,

downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

- q. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;
 - r. All records pertaining to the types of service used;
 - s. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and
 - t. Records related to all files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web

pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of James BUSHEY to the fingerprint scanner of the device; (2) hold a device found in front of the face of James BUSHEY and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.